Workaround Solution

Soal ini juga merupakan memory forensics, sequel dari Forget It.

Langkah-langkah solusinya adalah sebagai berikut:

1. Mengenali memory dump
2. Menentukan process of interest
3. Melakukan dump memory yang secara khusus dipakai oleh process of interest.
4. Mendapatkan flagnya

Mengenali memory dump

Sama seperti soal sebelumnya, kita perlu mengenali dumpnya. Walaupun di deskripsi ditulis machine apa, tapi jaga-jaga saja.

```
python vol.py -f <lokasi file> imageinfo
```

```
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86_24000, Win7SP1x86 (Instantiated with Win7SP1x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/mnt/f/CTF/soal araCTF/forensik2final/dump2.raw)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82786de8L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x80b96000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2021-01-31 05:24:26 UTC+0000
     Image local date and time : 2021-01-30 21:24:26 -0800
```

Yep, sama. Windows 7 SP1 32-bit.

Menentukan process of interest

Lakukan identifikasi proses yang sedang berjalan dengan command line berikut:

```
python vol.py -f <lokasi file> --profile=Win7SP1x86 cmdline
```

```
**************************************************************************
explorer.exe pid:   2320
Command line : C:\Windows\Explorer.EXE
**************************************************************************
SearchIndexer. pid:   2608
Command line : C:\Windows\system32\SearchIndexer.exe /Embedding
**************************************************************************
svchost.exe pid:   3232
Command line : C:\Windows\System32\svchost.exe -k secsvcs
**************************************************************************
svchost.exe pid:   3980
Command line : C:\Windows\System32\svchost.exe -k swprv
**************************************************************************
wuauclt.exe pid:   3048
Command line : "C:\Windows\system32\wuauclt.exe"
**************************************************************************
svchost.exe pid:   3484
Command line : C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
**************************************************************************
WmiPrvSE.exe pid:    336
Command line : C:\Windows\system32\wbem\wmiprvse.exe
**************************************************************************
iexplore.exe pid:   2904
Command line : "C:\Program Files\Internet Explorer\iexplore.exe"
**************************************************************************
TrustedInstall pid:   1860
Command line : C:\Windows\servicing\TrustedInstaller.exe
**************************************************************************
iexplore.exe pid:   3872
Command line : "C:\Program Files\Internet Explorer\iexplore.exe" SCODEF:2904 CREDAT:3814552 /prefetch:2
**************************************************************************
MsSpellCheckin pid:    472
Command line : "C:\Windows\System32\MsSpellCheckingFacility.exe" -Embedding
**************************************************************************
DumpIt.exe pid:   1900
Command line : "C:\Users\IEUser\Downloads\DumpIt.exe"
**************************************************************************
conhost.exe pid:    592
Command line : \??\C:\Windows\system32\conhost.exe "-848268847187609128510441126O9-924383991-478803685-1575714761-8121931591588369170
```

Tidak banyak yang terjadi. Yang dinyalakan user hanyalah Internet Explorer dan explorer.exe. Dalam soal ini, proses yang menjadi process of interest adalah **Internet Explorer**. Apa yang sekarang dilakukan oleh user di Internet Explorer? Sama seperti solusi alternatif dari Forget It, karena semua yang memiliki UI pasti masuk ke memory, maka kita dapat melakukan dump memory khusus pada Internet Explorer dan memproses UI dari itu.

Melakukan dump memory yang secara khusus dipakai oleh process of interest

Lakukan command volatility berikut ini.

PID dari Internet Explorer adalah 2904 dan 3872. Yang manapun seharusnya tak masalah, tapi untuk solusi ini menggunakan 3872.

```
python vol.py -f <lokasi file> --profile=Win7SP1x86 memdump -p 3872 -D <lokasi directory output>
```

File 3872.dmp muncul di directory output. Kemudian masukkan file ini ke GIMP dengan cara membuka GIMP > File > Open... kemudian masuk ke directory output, centang pilihan Show All Files dan pada menu Select File Type pilih Raw Image Data.

Scroll parameter Offset dan naikkan sedikit parameter Width. Umumnya dalam dump memory, bagian yang banyak memiliki warna solid adalah bagian UI yang dimaksud.

Mendapatkan flagnya

Setelah berkelana sedikit, terdapat sebuah UI yang dapat dicerna.

Flag:

```
ara2021{I_STILL_CANT_ROTATE_TEXT_HERE}
```